Cookies in a honeypot: the illusion of data privacy in the U.S.

Author: Kiana Dane
Computing ID: Urn8he

What we allow to get stolen

While browsing reading selections in September, there it was: another "listicle" – an article formatted as a list of "top events" in a certain category with a sensational title that entices a reader to visit a webpage by teasing them with entertaining, digestible content. In CSO's "The 18 biggest data breaches of the 21st century," breach number four is by a firm who provides a service I know and love. "In 2021, networking giant LinkedIn saw data associated with 700 million of its users posted" [2] by a hacker calling themselves 'God User.' LinkedIn argued that no sensitive personal or private data was exposed in the leak, but "God User" countered that claim by posting a data sample that "contained… email addresses, phone numbers, geolocation records… and other social media details".

For many LinkedIn users, this came as a "red flag" and called into question the firm's responsibility as an ethical steward of personal data. Personally, while I cannot trust LinkedIn to keep my phone number or geolocation records safe, I still opt to share both pieces of data with the digital platform in exchange for the benefit I get by doing so while using it.

How we define consent and processing

To borrow a definition from the General Data Protection Regulation (GDPR) law passed by the European Union in 2018, data processing occurs when a firm collects, records, organizes, stores, or uses data [4]. A user's consent for a firm to process their personal data is based on a relationship of trust, between the user and the firm, that the firm will act in a user's best interest regarding use of that data (e.g. refraining from distributing it to third parties, especially for financial gain). However, when firms offer services (especially via hosted digital platforms) that dominate the market, their data governance policies often exploit that user consent, and ultimately harm the user, to create more value for themselves [3].

How we define Privacy

In the United States, the definition of "privacy" when it comes to data collected from internet users is widely variable and still evolving. Kirsten Martin argues that courts have taken shortcuts to define privacy in ways that "justify platforms creating an attractive customer-facing platform to lure in customers and later exploit user data in a secondary platform or business." She calls this problem "the honeypot problem" [3].

In her essay, Martin identifies one of these shortcuts as being the definition of "privacy as concealment." This defines personal information "as 'private' when concealed and 'not private' when seen or shared. Disclosed information, since not private, has no rules… as to how [it] will be stored, used, or shared" [3]. To highlight the danger of this shortcut, Martin turns to a case settled in 2022 in the U.S. Court of Appeals for the Ninth Circuit.

Back to LinkedIn

In *hiQ Labs v. LinkedIn*, the court ruled that LinkedIn users voluntarily offer their data to be seen and shared, so they must not have an interest in the privacy of that data. This sets the precedent that 1) "[firms] are not obligated to respect privacy interests of their users after collecting their data" and 2) businesses like hiQ should continue to "be allowed access to

LinkedIn users' posts in order to develop their own business, since users (supposedly) have no interest in that data" [3]. These precedents threaten to undermine the autonomy of users by allowing firms to take control of their personal information. Firms have a responsibility to act as ethical data stewards, ensuring that their actions prioritize societal well-being over short-term profits.

So, what can we do?

Firms should continue to press United States courts for definitions of privacy that benefit all parties, and users should continue to press firms to be transparent and forthcoming about their governance policies. Additionally, users in the U.S. should vote for representatives that value data privacy and support government policies that echo the values of the EU's GDPR law. Politicians should look to the GDPR as a value framework and support policies such as 1) mandating that user consent must be "freely given, specific, informed and unambiguous," 2) mandating that requests for consent must be presented in "clear and plain language," and 3) protecting users by affirming their right to "withdraw previously given consent whenever they want" [4].

Works Cited

1. Faverio, Michelle. “What the Data Says about Americans’ Views of Artificial Intelligence.” *Pew Research Center*, Pew Research Center, 21 Nov. 2023, www.pewresearch.org/short-reads/2023/11/21/what-the-data-says-about-americans-views-of-artificial-intelligence/.

2. Leyden, John, et al. “The 18 Biggest Data Breaches of the 21st Century.” *CSO Online*, CSO, 12 Sept. 2024, www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html.

3. Martin, Kirsten. “Platforms, Privacy & the Honeypot Problem.” *https://Jolt.Law.Harvard.Edu/*, Harvard Journal of Law and Technology, 21 Dec. 2023, jolt.law.harvard.edu/assets/articlePDFs/v37/Symposium-5-Martin-Platforms-Privacy-and-the-Honeypot-Problem.pdf.

4. Wolford, Ben. “What Is GDPR, the EU’s New Data Protection Law?” *GDPR.Eu*, Proton Technologies AG, 7 Nov. 2018, gdpr.eu/what-is-gdpr/.